an exclusive-OR element for calculating an exclusive-OR of a constant determined for each of the key transform devices and a first key obtained from the input key;

a nonlinear transform unit for nonlinearly transforming an output from the exclusive-OR element using a predetermined substitution table;

an expansion unit for performing an expansion processing on an output from the nonlinear transform unit; and

an expansion key calculation unit for calculating the expansion key based on an output from the expansion unit and a second key obtained from the input key.

A1

28. (NEW) The expansion key generation apparatus according to claim 27, wherein each of the key transform devices further comprises:

a rotation unit for shifting the input key to a least significant bit or a most significant bit and inputting the shifted key to the key transform device of a next stage.

29. (NEW) The expansion key generation apparatus according to claim 28, wherein a shift amount of the rotation unit is relatively prime to the number of output bits of the nonlinear transform unit.

30. (NEW) The expansion key generation apparatus according to claim 27, wherein the expansion unit performs a shifting of a predetermined number of bits.

31. (NEW) The expansion key generation apparatus according to claim 30, wherein the expansion unit shifts the output from the nonlinear transform unit to the least significant bit by the number of bits that is half the number of bits of the output from the nonlinear transform unit, or by the number of bits obtained by adding an integer multiple of the number of bits of the output from the nonlinear transform unit to the half number of bits.

32. (NEW) The expansion key generation apparatus according to claim 27, wherein the expansion key calculation unit adds with carry-up the output from the expansion unit and the second key.

A1

33. (NEW) An encryption and decryption apparatus comprising an expansion key generation apparatus according to claim 27, comprising:

a data randomization unit for ciphering a plaintext to obtain a cipher text or deciphering a cipher text to obtain a plaintext by processing an input text by a round function based upon the expansion keys generated by the key transform devices.

34. (NEW) The encryption and decryption apparatus according to claim 33, wherein the data randomization unit uses a plurality of substitution tables for encryption and decryption, and the plurality of substitution tables are common to the predetermined substitution table of the nonlinear transform unit.

35. (NEW) An expansion key generation method, which generates expansion keys based on input keys using a plurality of cascade-connected key transform devices, each of the key transform devices generating the expansion keys by a method comprising:

calculating an exclusive-OR of a constant determined for each of the key transform devices and a first key obtained from the input key;

nonlinearly transforming a result of an exclusive-OR using a predetermined substitution table;

A1

performing an expansion processing on a result of a nonlinear transform; and

calculating the expansion key based on a result of expansion processing and a second key obtained from the input key.

36. (NEW) An expansion key generation program, which causes a computer to generate expansion keys based on input keys using a plurality of cascade-connected key transform devices, the program comprising:

program code for calculating an exclusive-OR of a constant determined for each of the key transform devices and a first key obtained from the input key;

program code for nonlinearly transforming a result of an exclusive-OR using a predetermined substitution table;

program code for performing an expansion processing on a result of a nonlinear transform; and

program code for calculating the expansion key based on a result of expansion processing and a second key obtained from the input key.

37. (NEW) An expansion key generation program, which causes a computer to generate expansion keys based on input keys using a plurality of cascade-connected key transform devices, the program comprising:

program code for calculating an exclusive-OR of a constant determined for each of the key transform devices and a first key obtained from the input key;

program code for nonlinearly transforming a result of an exclusive-OR using a predetermined substitution table;

A1

program code for performing an expansion processing on a result of a nonlinear transform;

program code for calculating the expansion key based on a result of expansion processing and a second key obtained from the input key; and

program code for shifting the input key to a least significant bit or a most significant bit and inputting the shifted key to the key transform device of a next stage.

38. (NEW) The program according to claim 37, wherein the program code for shifting the input key comprises program code for shifting the input key by a relatively prime to the number of output bits of a result of a nonlinear transform.

39. (NEW) The program according to claim 37, wherein the program code for performing an expansion processing comprises program code for shifting a result of a nonlinear transform by a predetermined number of bits.

40. (NEW) The program according to claim 39, wherein the program code for performing an expansion processing comprises program code for shifting a result of a nonlinear transform by the number of bits that is half the number of bits of a result of a nonlinear transform, or by the number of bits obtained by adding an integer multiple of the number of bits of the result of the nonlinear transform to the half number of bits.

A1

41. (NEW) The program according to claim 36, wherein the program code for calculating the expansion key comprises program code for adding with carry-up a result of an expansion and the second key.

42. (NEW) The program according to claim 36, further comprising:

program code for ciphering a plaintext to obtain a cipher text or deciphering a cipher text to obtain a plaintext by processing an input text by a round function based on the generated expansion keys.

43. (NEW) The program according to claim 42, wherein the program code for ciphering or deciphering comprises program code for randomizing the plaintext or the cipher text by using a plurality of substitution tables for encryption and decryption, the plurality of substitution tables being common to the predetermined substitution table.

44. (NEW) An expansion key generation apparatus comprising:

a plurality of cascade-connected key transform devices for receiving different keys and generating expansion keys based on the received keys, each of the key transform devices comprising a plurality of parallel devices, each of the parallel devices comprising:

a register for storing a constant determined for each of the parallel devices;

an exclusive-OR element for calculating an exclusive-OR of the constant stored in the register and a first key obtained from the received key;

A1

a substitution unit for converting an output from the exclusive-OR element using a predetermined substitution table; and

an expansion unit for performing an expansion processing on an output from the substitution unit; and

an expansion key calculation unit for calculating the expansion key based on an output from the expansion unit and a second key obtained from the input key.

45. (NEW) An expansion key generation program, which causes a computer to generate expansion keys based on input keys using a plurality of cascade-connected key transform devices that receive different keys and generate expansion keys based on the received keys, each of the key transform devices comprising a plurality of parallel devices, the program comprising:

program code for storing a constant determined for each of the parallel devices;

program code for calculating an exclusive-OR of the constant stored in the register and a first key obtained from the received key;

program code for converting an output from the exclusive-OR element using a predetermined substitution table;

program code for performing an expansion processing on an output from the substitution unit; and

program code for calculating the expansion key based on a result of an expansion and a second key obtained from the input key.

46. (NEW) An expansion key generation apparatus comprising:

A1
concl.

a plurality of cascade-connected key transform devices for generating expansion keys based on input keys, each of the key transform devices comprising:

a first key transform unit for nonlinearly transforming a first key obtained from the input key using a predetermined substitution table;

an expansion key calculation unit for calculating the expansion key based on an output from the first key transform unit and a second key obtained from the input key; and

a rotation unit for shifting the input key to a least significant bit or a most significant bit and inputting the shifted input key to the key transform device of a next stage, wherein a shift amount of the rotation unit is relatively prime to the number of output bits of the first key transform unit.